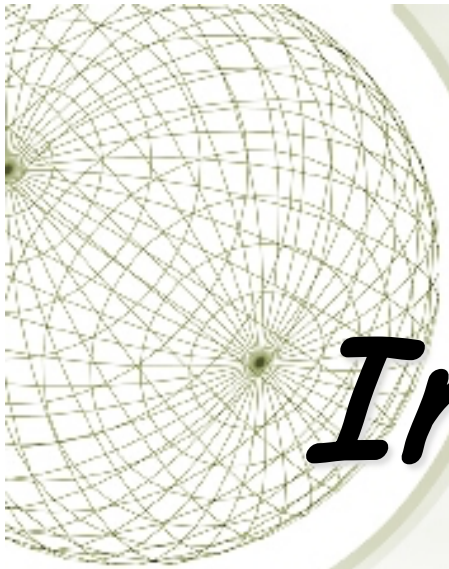
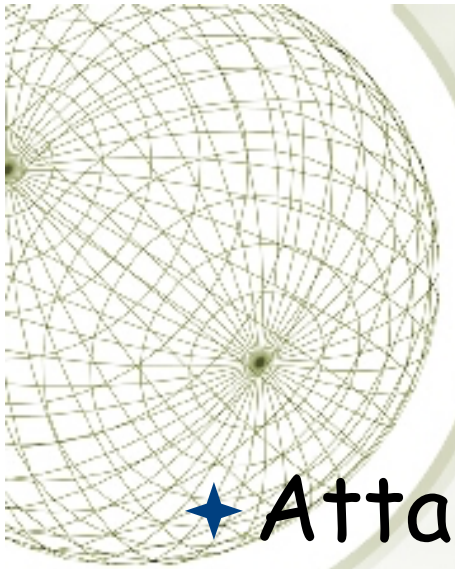


Internet Security

Ola Flygt
Linnaeus University, Sweden
http://homepage.lnu.se/staff/oflmsi/
Ola.Flygt@lnu.se



Outline

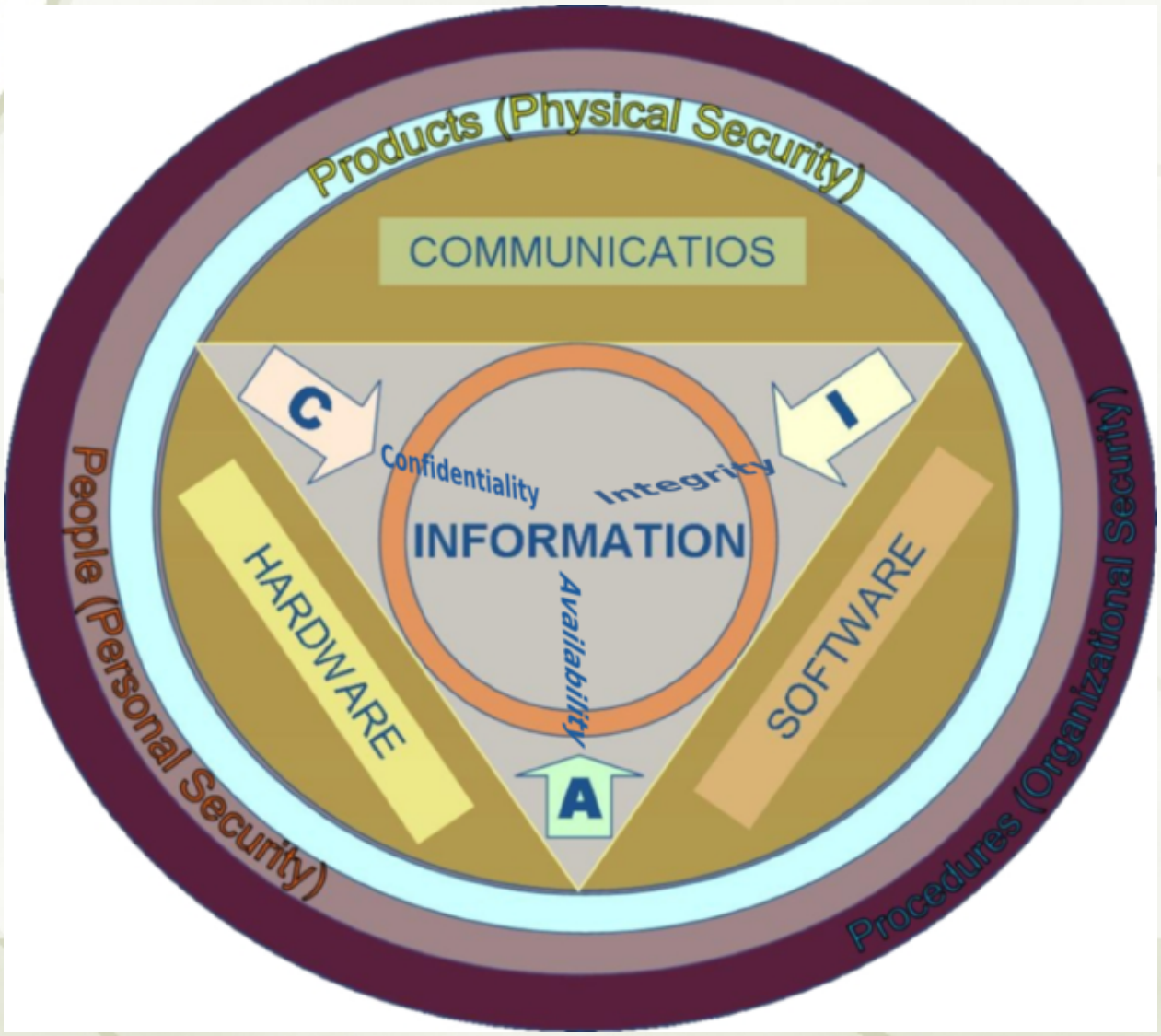
- Attacks, services and mechanisms
- Security attacks
- Security services
- Methods of Defence
- Models for Internetwork Security
- Internet standards and RFCs

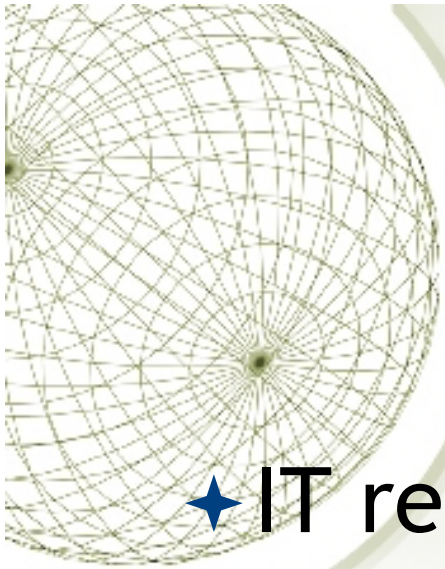
Security

- "When we know our surroundings and have tools to protect ourselves, we can feel more secure."
- "It makes me feel secure to be around my dog. He will always warn me if something is wrong."
- "Knowing someone is looking out for me is what security means to me."
- "If we did not have security, our world would be a very bad place."

("What Security Means To Me" essays at www.panasonic.com/security.)

Information Security





The Security Landscape

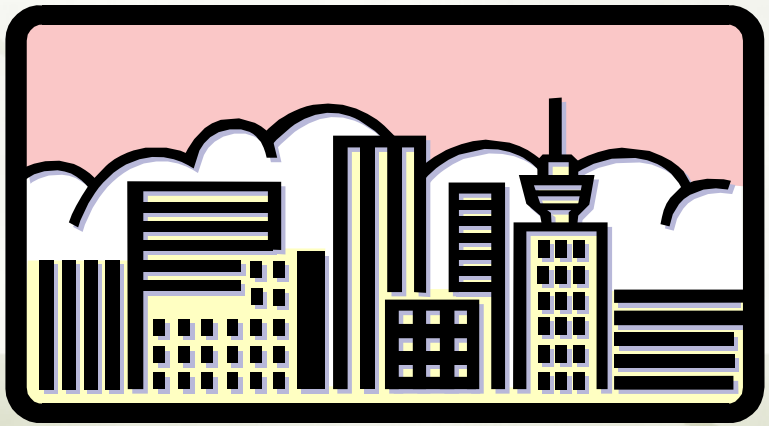
- IT realm
- Physical realm
  - Airport
  - Food security, etc.
- Political realm
  - International etc.
- Monetary realm
  - Financial, etc.

The IT Security Landscape

- Computing security
- Data security
- Application security
- Information security
- Network security

OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study



Aspects of Security

- **Security Attack:** Any action that compromises the security of information.
- **Security Service:** A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.
- **Security Mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack.

Security Attacks

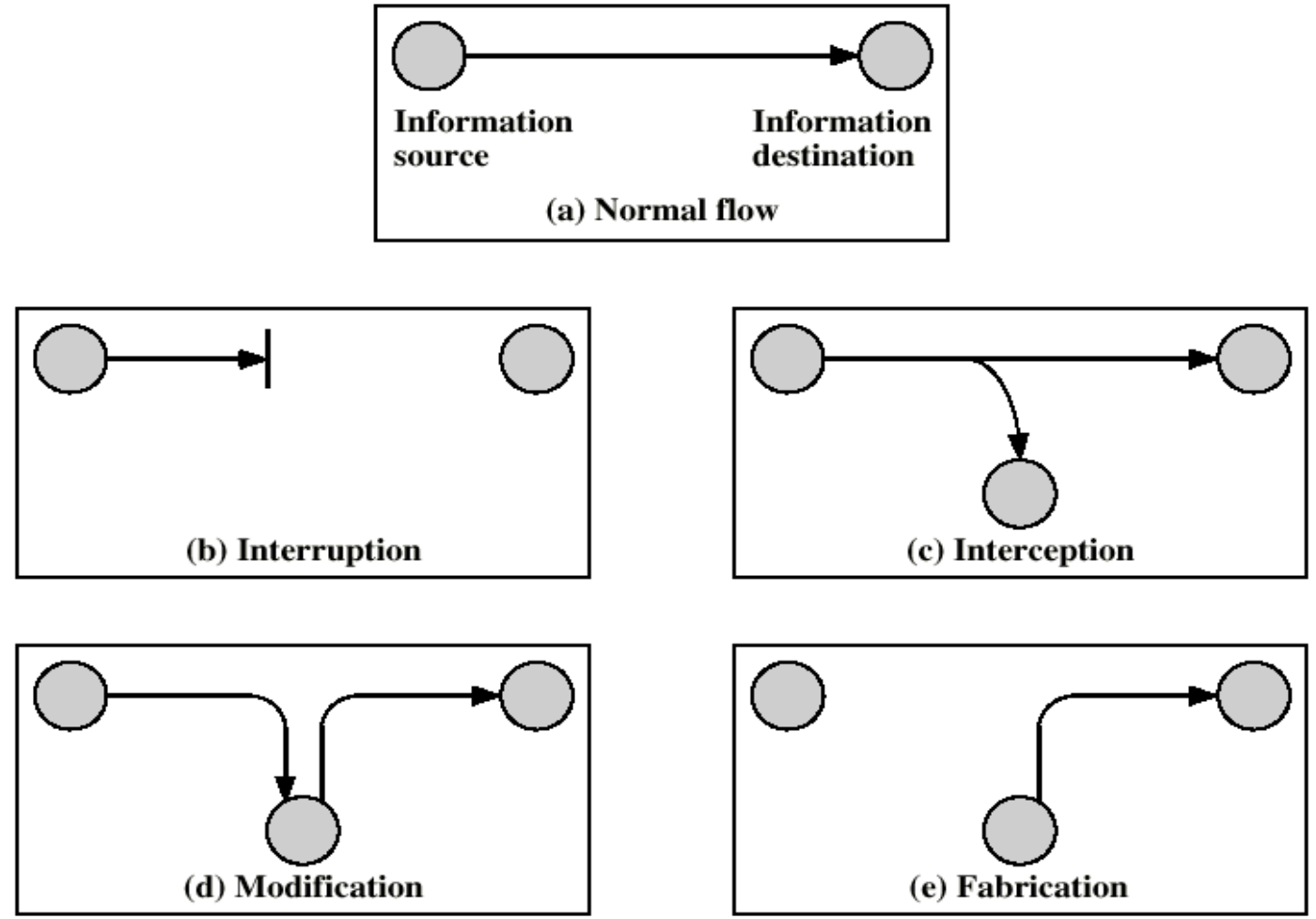
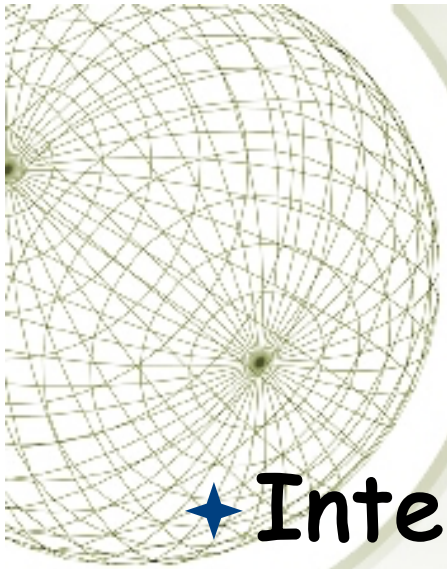


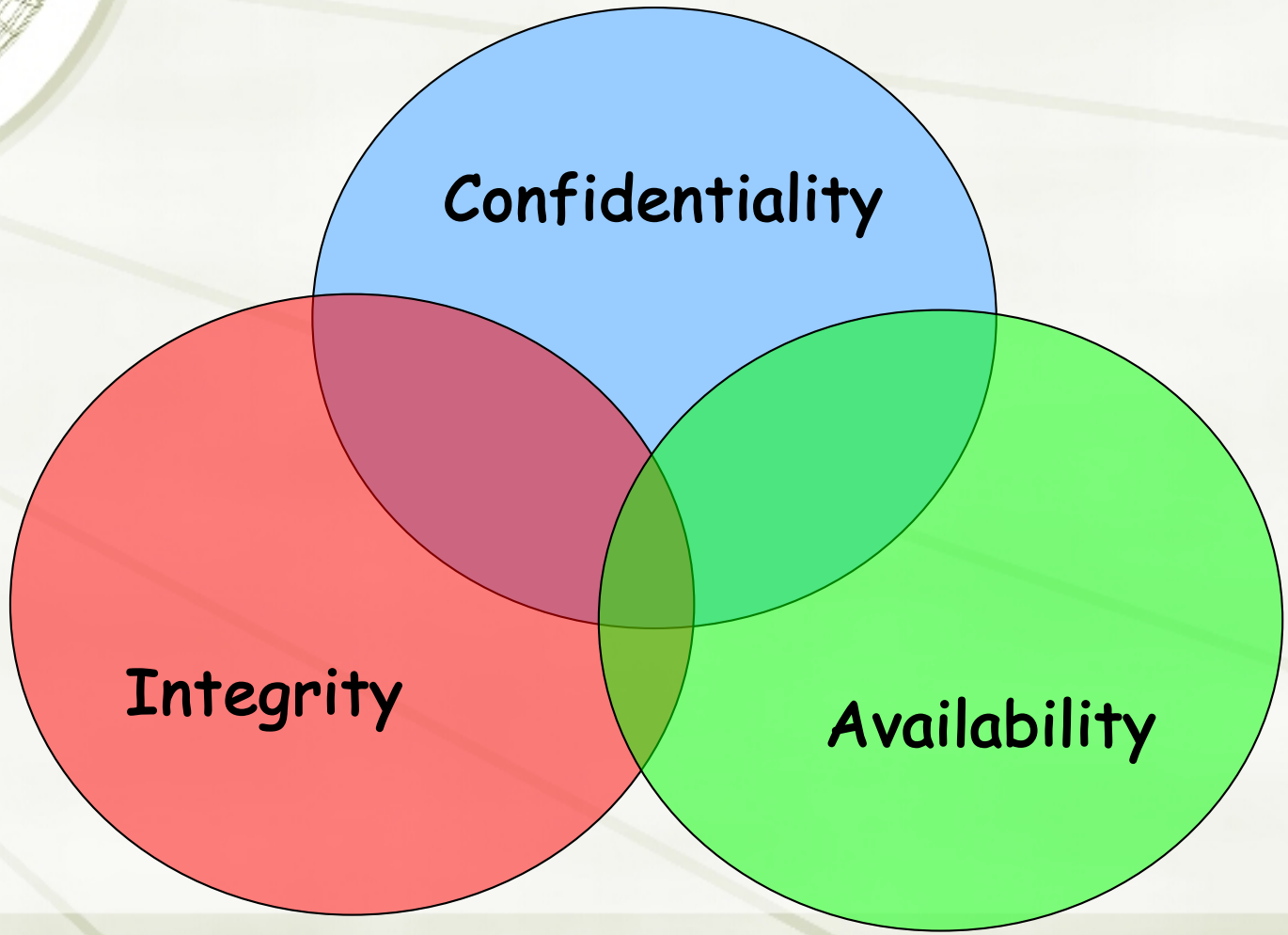
Figure 1.1 Security Threats

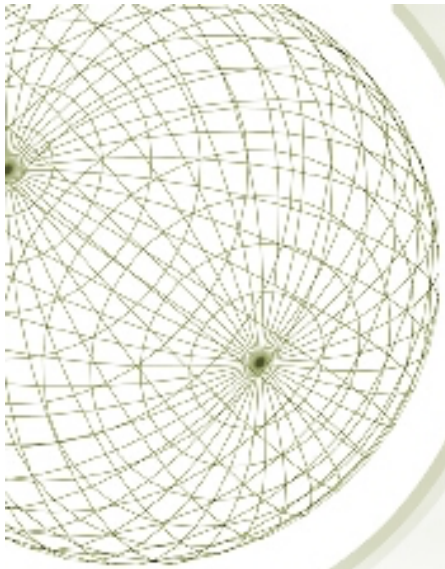


Security Attacks

- **Interruption:** This is an attack on availability
- **Interception:** This is an attack on confidentiality
- **Modification:** This is an attack on integrity
- **Fabrication:** This is an attack on authenticity

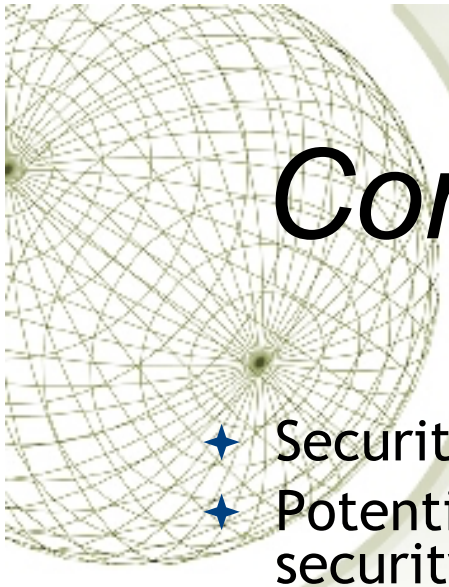
Security Goals





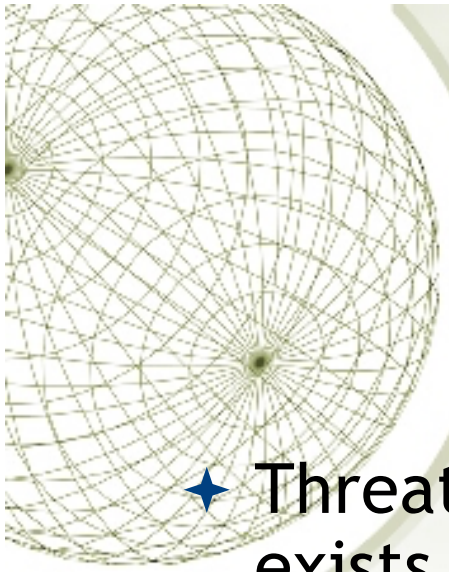
Examples of Security Requirements

- confidentiality – student grades
- integrity – patient information
- availability – authentication service



Computer Security Challenges

- Security is not simple
- Potential attacks on the security features need to be considered
- Procedures used to provide particular services are often counter-intuitive
- It is necessary to decide where to use the various security mechanisms
- Requires constant monitoring
- Is too often an afterthought
- Security mechanisms typically involve more than a particular algorithm or protocol
- Security is essentially a battle of wits between a perpetrator and the designer
- Little benefit from security investment is perceived until a security failure occurs
- Strong security is often viewed as an impediment to efficient and user-friendly operation



Threats and Attacks

- Threat: A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a **threat** is a possible danger that might exploit a **vulnerability**.
- Attack: An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Types of Threats

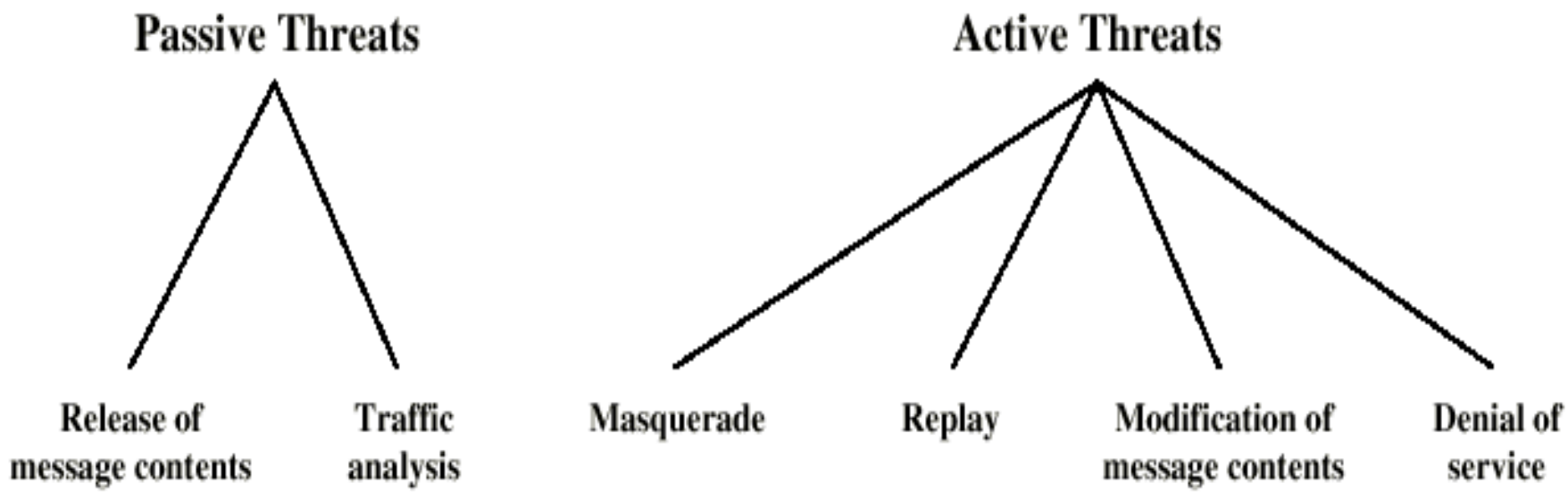
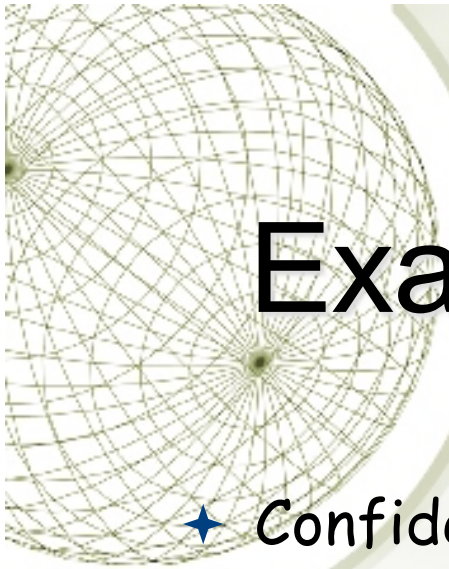


Figure 1.2 Active and Passive Security Threats

Security Service (X.800)

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

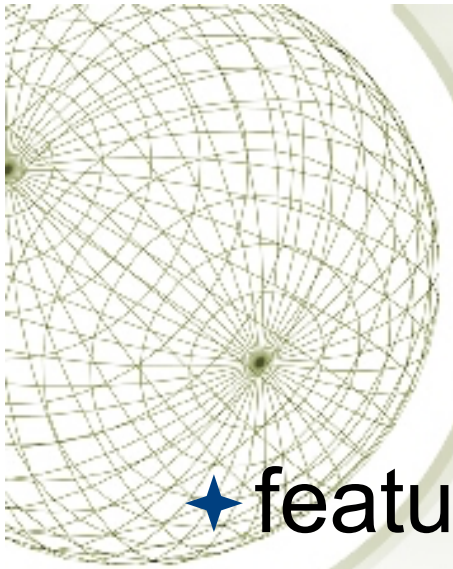


Example of Security Services

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (you can not deny sending or receiving some information)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

Security Service vs Attack

	Attack					
Service	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Peer entity authentication			Y			
Data origin authentication			Y			
Access control			Y			
Confidentiality	Y					
Traffic flow confidentiality		Y				
Data integrity				Y	Y	
Non-repudiation						
Availability						Y



Security Mechanism

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**
- hence our focus on this topic

Example of Security Mechanisms

- Encipherment
- Digital Signature
- Access Control
- Authentication Exchange
- Traffic Padding

And more…..

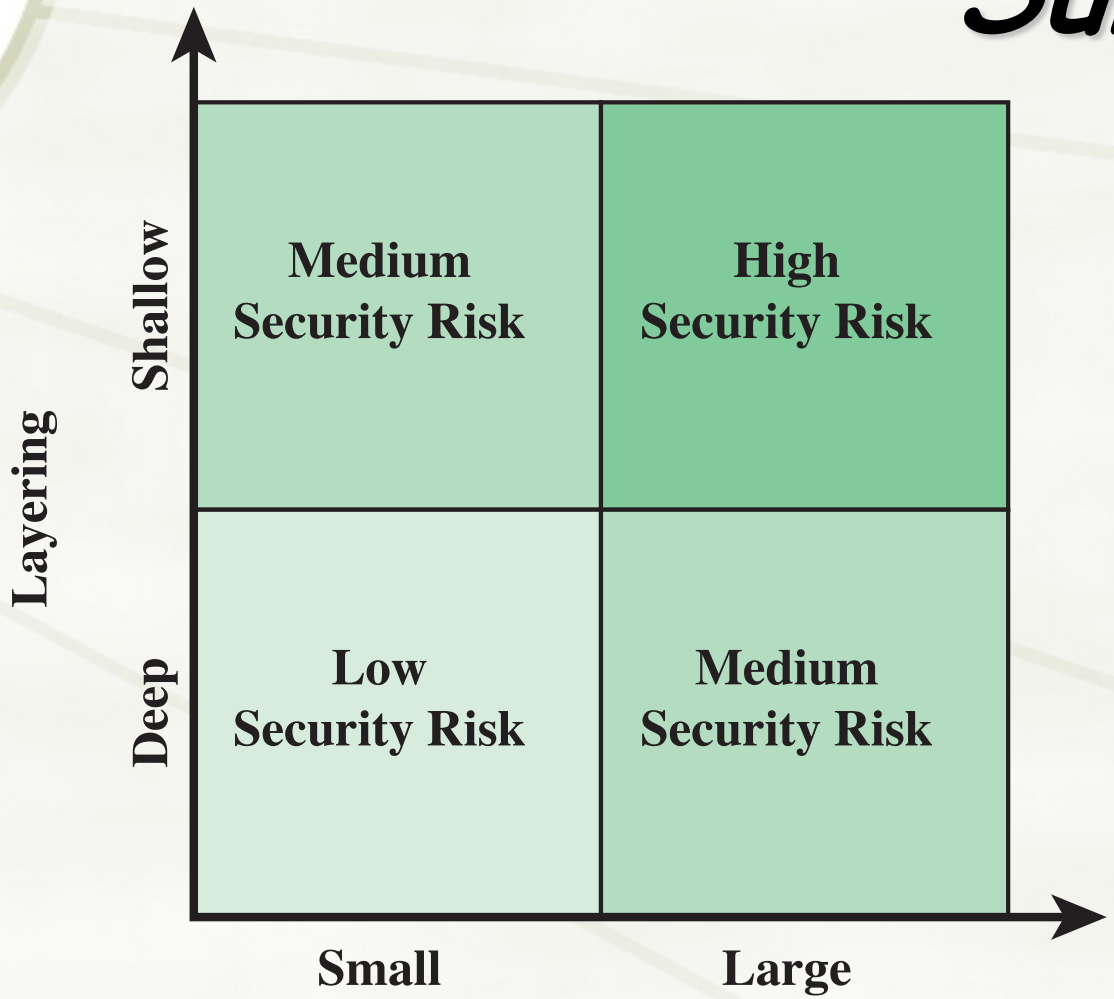
Service vs Mechanisms

Service	Mechanism							
	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Attack Surface

- Consists of the reachable and exploitable vulnerabilities in a system
  - Examples:
    - Open ports on outward facing Web and other servers, and code listening on those ports
    - Services available on the inside of a firewall
    - Code that processes incoming data, e-mail, XLM, office documents, and industry-specific custom data exchange formats
    - Interfaces, SQL, and Web forms
    - An employee with access to sensitive information vulnerable to a social engineering attack
- Can be categorized in the following way:
  - Network attack surface
    - This category refers to vulnerabilities over an enterprise network, wide-area network, or Internet
  - Software attack surface
    - Vulnerabilities in application, utility, or operating system code
  - Human attack surface
    - Refers to vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

Defence in depth and Attack Surface



Attack trees

A branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities

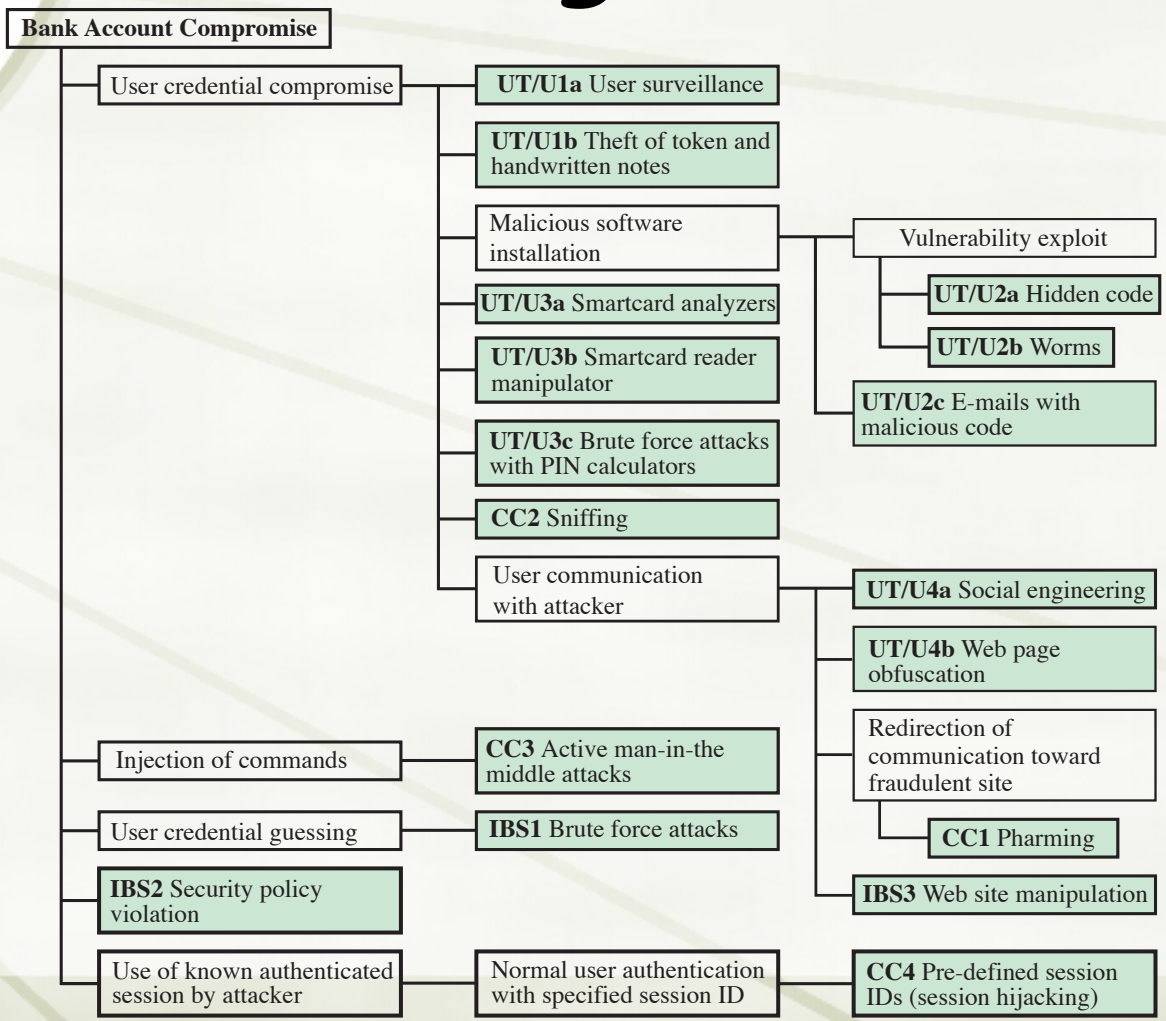
The security incident that is the goal of the attack is represented as the root node of the tree

The ways that an attacker could reach that goal are iteratively and incrementally represented as branches and subnodes of the tree

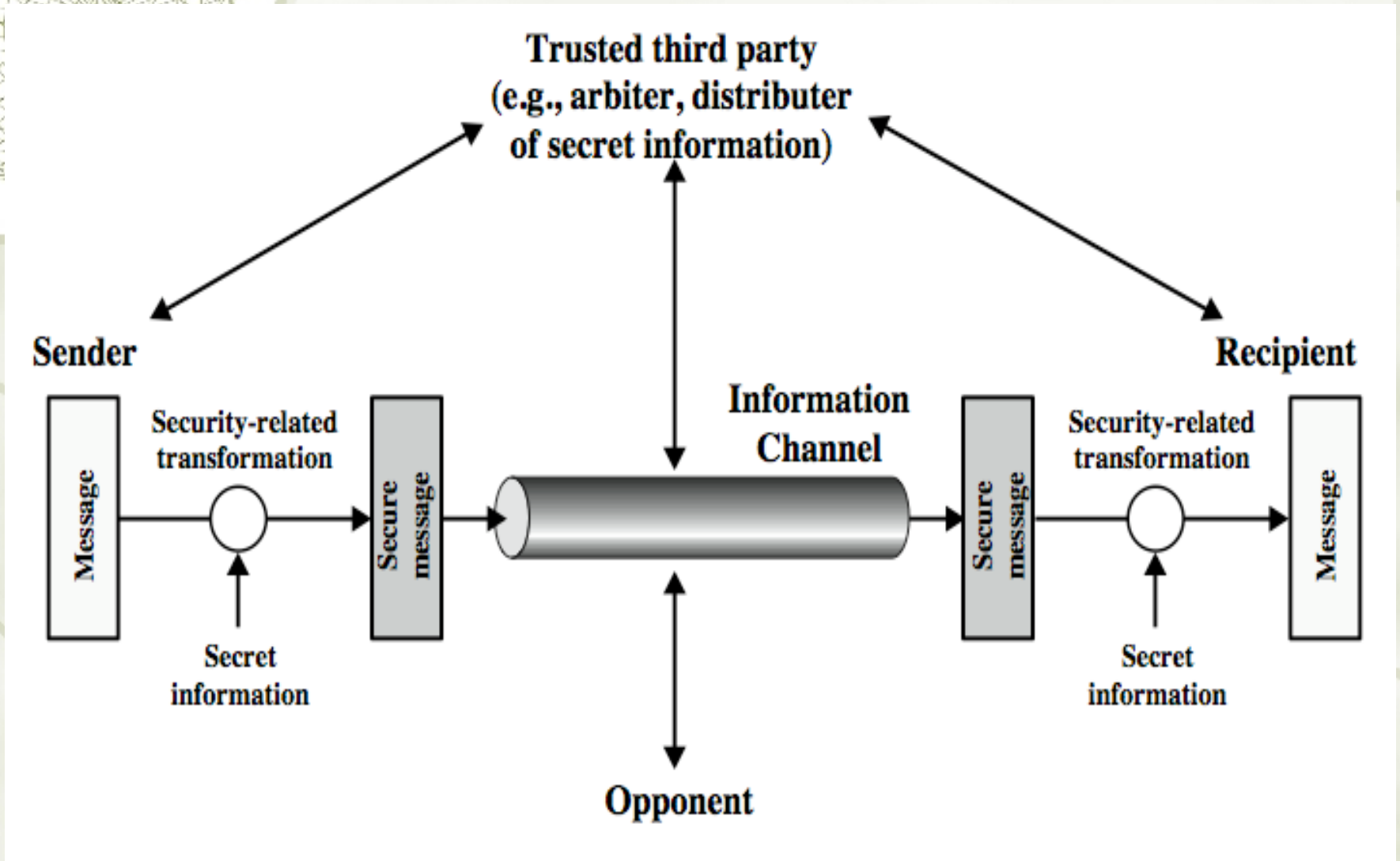
The final nodes on the paths outward from the root, the leaf nodes, represent different ways to initiate an attack

Branches can be labeled with values representing difficulty, cost, or other attack attributes, so that alternative attacks can be compared

An Attack Tree for Internet banking Authentication



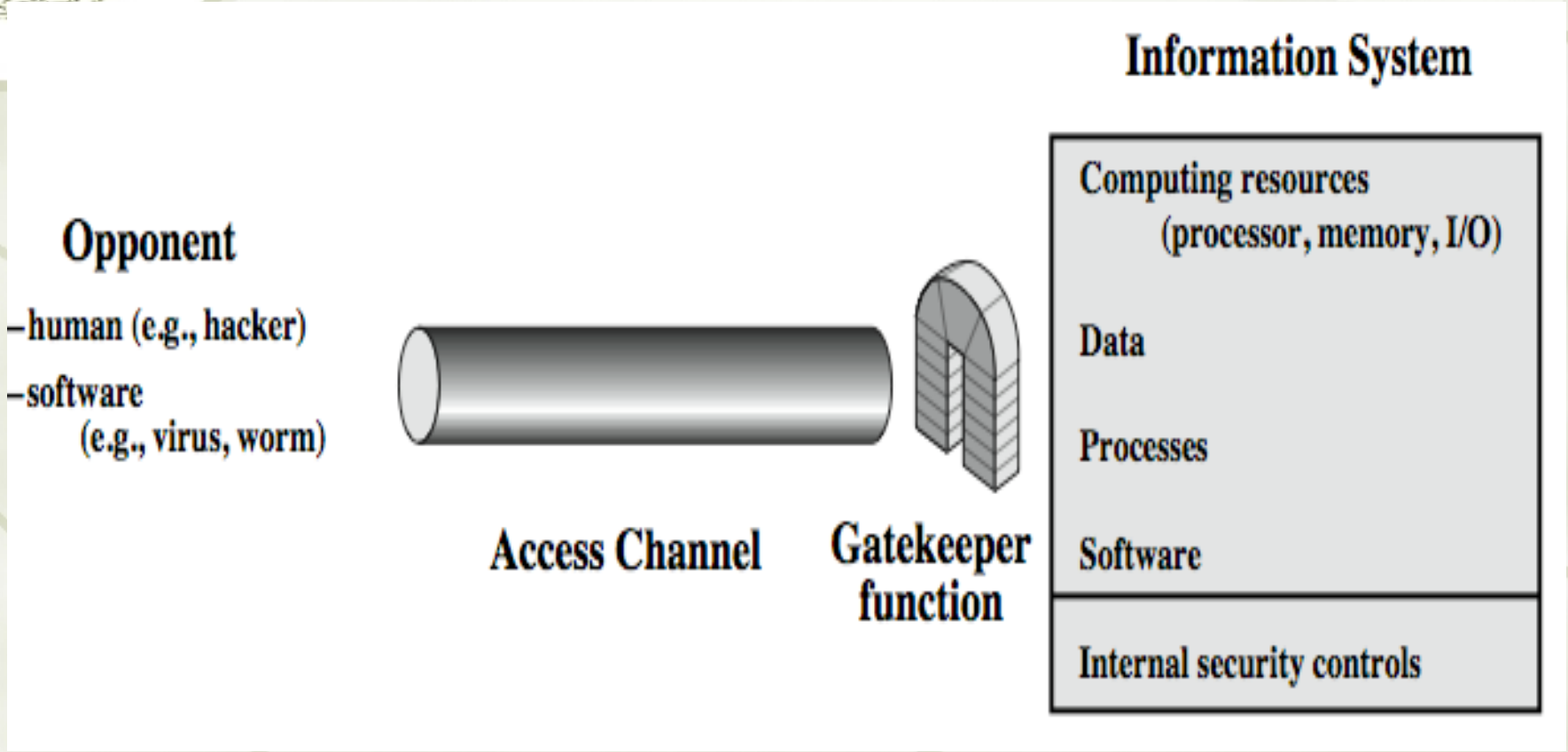
Model for Network Security

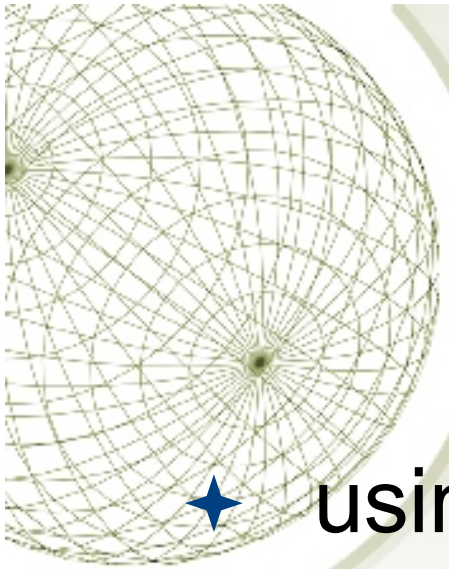


Model for Network Security

- using this model requires us to:
  1. design a suitable algorithm for the security transformation
  2. generate the secret information (keys) used by the algorithm
  3. develop methods to distribute and share the secret information
  4. specify a protocol enabling the principals to use the transformation and secret information for a security service

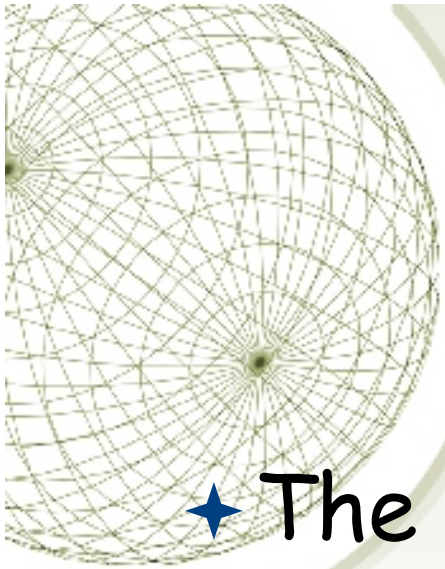
Model for Network Access Security





Model for Network Access Security

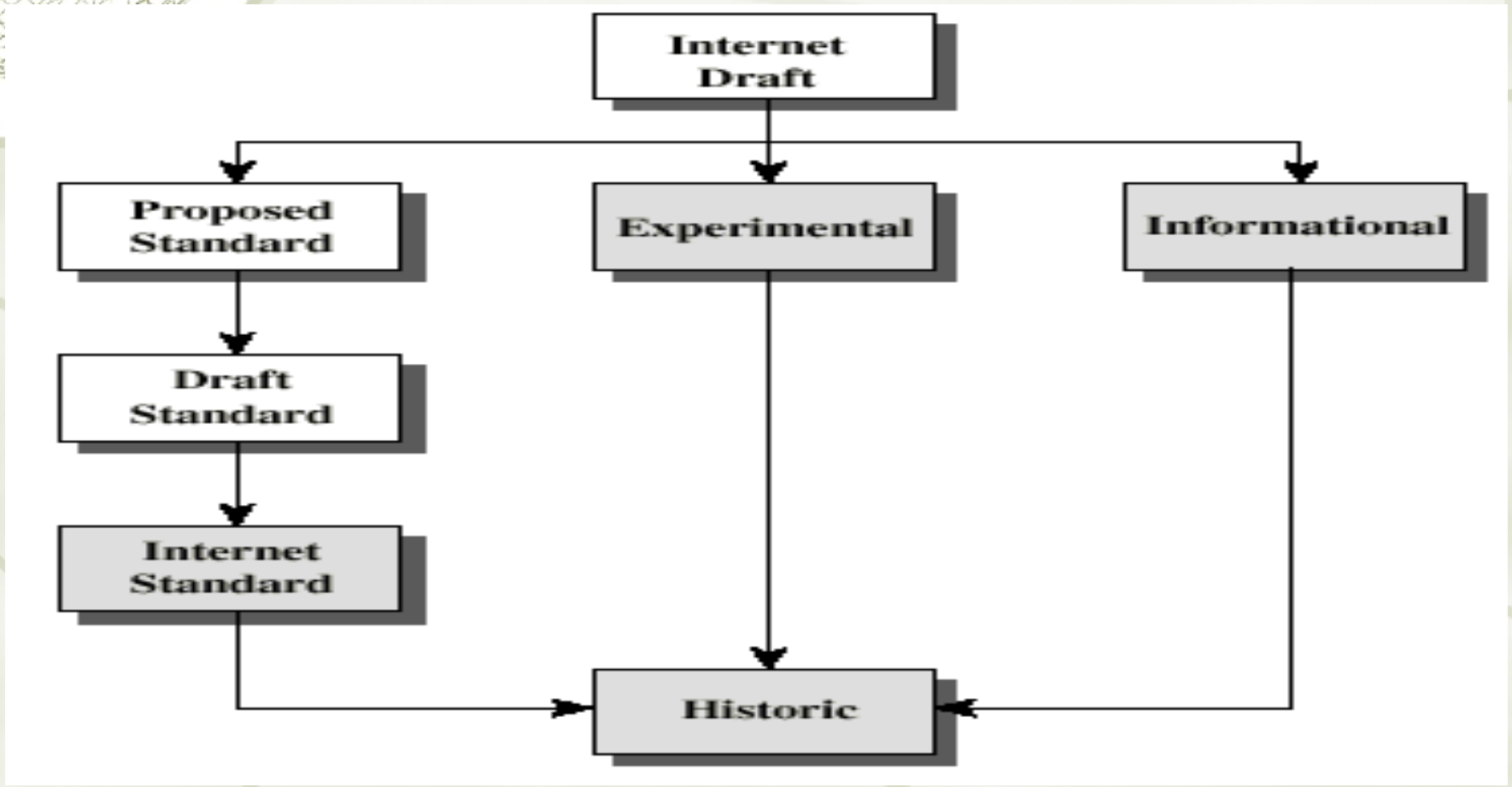
- using this model requires us to:
  1. select appropriate gatekeeper functions to identify users
  2. implement security controls to ensure only authorised users access designated information or resources

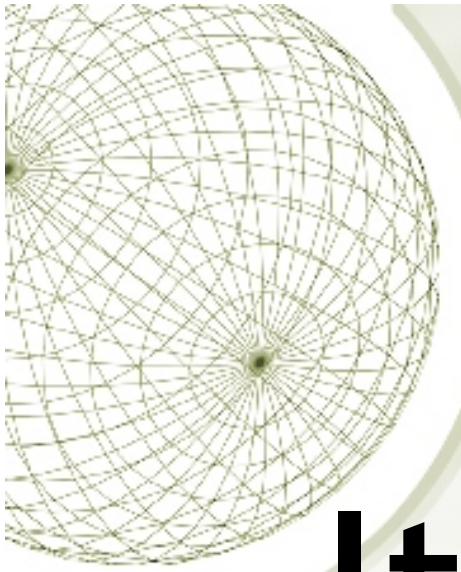


Internet standards

- The Internet society (ISOC)
  - Internet Architecture Board (IAB)
    - Internet Engineering Steering Group (IESG)
    - Internet Engineering Task Force (IETF)
      - working groups and informal discussion groups
  - Internet Assigned Numbers Authority (IANA)
- National Institute of Standards and Technology (NIST)

Internet RFC Publication Process





It’s time for a Kahoot!